

Criminal Evidences Management System Using Blockchain

¹K.Vijay Kumar ,²K.Manimala ,³A.Venkat Ramreddy ,⁴A.Ganapathi ,⁵A.Aravind
¹Associate Professor,Department of Computer Science and Enginneering(AI&ML)
vijaykumar@cmritonline.ac.in

²Assistant Professor,Department of Computer Science and Enginneering(AI&ML)
manimala@cmritonline.ac.in

³Department Of Computer Science and Engineering (AI&ML), CMRIT
Hyderabad, Telangana, India
22r017368@cmrithyderabad.edu.in

⁴Department Of Computer Science and Engineering (AI&ML), CMRIT
Hyderabad, Telangana, India
22r01a7369@cmrithyderabad.edu.in

⁵Department Of Computer Science and Engineering (AI&ML), CMRIT
Hyderabad, Telangana, India
22r01a7371@cmrithyderabad.edu.in

ABSTRACT

Criminal Evidence Management System based on the Blockchain is created to address the issue of evidence-tampering in the police systems. In normal systems, evidence is stored at a central database and it can be modified or at times deleted by hackers or corrupt individuals. This may bring about unfairness in the judiciary. In order to address this issue, Blockchain technology is employed in this project and data are stored in numerous computers rather than a single server. When evidences are stored in blockchain, there is no easy way to change or destroy them. All records are stored using a unique hash code, hence in the event, one attempts to alter the information, then this will be immediately detected. The system operates on Smart Contracts which are coded in Solidity to handle evidence. It has various users such as Admin and Police Officers. Records can be viewed and added by the admin and uploaded and viewed by the officers in a secure place. The system enhances security, transparency and trust in the criminal investigations. It makes evidence secure, original and trustworthy in the court, which is how justice system should operate.

Keywords-

- Blockchain
- Criminal Evidence
- Evidence Management System
- Smart Contracts
- Solidity
- Ethereum
- IPFS
- Chain of Custody
- Data Security
- Tamper-proof Storage
- Decentralized System
- Police Investigation System

I. INTRODUCTION

Evidence is quite significant in the criminal justice system in discovering the truth. Evidence may include photos, videos, fingerprints, documents or digital files that have been obtained at a crime scene. This is evidence upon which judges and police rely to determine whether an individual is guilty or not. Any manipulation of evidence, its loss, or destruction may cause wrongful decisions and injustice. Under the traditional systems, the criminal evidence is stored in databases or physical records that are located centrally. There are numerous issues with such systems. Hackers or corrupt employees

can make alterations in evidence records. Certainly, at times records are lost because of system failure or human error. In addition, it is challenging to monitor the individuals that accessed the evidence or handled it. Due to the mentioned problems, individuals might lose confidence in the investigation procedure. This project enjoys the use of Blockchain technology to address these issues. Blockchain is a distributed network, in which the information is stored in numerous computers rather than a single server. After the addition of data there is always no easy way of altering the data since the records have associated together with a unique hash code and time. When somebody attempts to alter the evidence, this

system identifies this. This renders storage of evidence to be secure, transparent and non-tamperable. Smart Contracts can also be used to manage evidence operations by the system. Smart contracts refer to programs that verify rules before undertaking such actions as adding or viewing evidence automatically. Only people with the right such as the police officers, forensic experts, and administrators have access to the system. This enhances protection and preservation of the chain of custody of evidence. Blockchain is used in this project along with other technologies such as Ethereum and IPFS to securely store and manage digital evidence. Admin users have the opportunity to create officer accounts, and the officers can create and view evidence without risks. All activities are logged in and this enhances responsibility and confidence in the system. In general, Criminal Evidence Management System based on Blockchain is a contemporary system of evidence management. It will assist in avoiding tampering of evidence, enhance transparency, and facilitate fair justice. This system might come in handy in future especially to police departments, forensic labs and courts.

II. RELATED WORK

The possibility of criminal and digital evidence protection through the help of Blockchain technology has been researched by many researchers. A study article described that blockchain would allow storing evidence in the form of a hash so that it would be impossible to alter it in the future. This assists in preserving the evidence in the chain of custody and safeguarding the evidence throughout investigation and trial. Another research was named SecureChain and suggested the introduction of a system in which digital evidence is exchanged safely among police, forensic professionals, and even courts. It employed smart contracts and role-based access such that only authorized individuals can access evidence. This enhances security and confidence to the system. There were also researchers who proposed blockchain-based structures to trace all the measures of evidence such as creation, accessibility, and transfer. Such systems make an open audit trail such that the investigators are able to know who touched the evidence and when easily. This cuts down on the tampering and human errors. One more piece of

work demonstrated the use of Ethereum smart contracts as permissions of evidence and logs. Other models go as far as to integrate blockchain with AI tools to assist in classifying and analyzing evidence in greater detail. Through all these researches, we get to know that blockchain proves to be highly effective in managing evidence that is secure, transparent and cannot be tampered with. Based on these studies, our Criminal Evidence Management System was created based on Blockchain.

III. METHODOLOGY

- User Registration and Login

First, every user is registered in the system such as Admin, Police Officers and Forensic Experts. The users receive usernames and passwords. The system can only be logged and used by authorized users. This prevents the loss of evidence in the hands of strangers.

- Adding Officer Details

Upon log-in, Admin includes officer details such as name, police station, and position. Such information is kept in blockchain in order not to be altered in the future. The officers are then provided with the details of logging into the system.

- Evidence Collection

In the event of a crime, evidence is gathered by police officers in the form of photos, videos, documents, or audio recordings. This evidence can be uploaded into the system without any risk.

- Evidence Upload

Officers input evidence on the system. The raw file is saved in a decentralized storage such as IPFS and a hash value is generated. This will be stored in blockchain. In case somebody modifies the file, the hash will be different and interference will be registered.

- Blockchain Recording

All evidence uploading, access, and transfer activities are registered in the blockchain ledger. The records

consist of a timestamp, user ID, and block number. This leaves an immortal history of the evidence.

- Smart Contract Execution

Smart contracts are automatically used to ensure the rules are checked prior to any action. As an example, evidence can only be uploaded by authorized officers. This eliminates human errors and enhances security.

- Role-Based Access Control

There are varying permissions of different users. The officers are able to upload the evidence, forensic experts are able to examine and the admin is able to monitor all records. This maintains the order of the system and makes it secure.

- Evidence Verification

Checking whether the evidence is original or not can be carried out by the users. The system will compare the blockchain hash and the current file hash. When both are identical, then there is no danger, and when they are different, tampering is recorded.

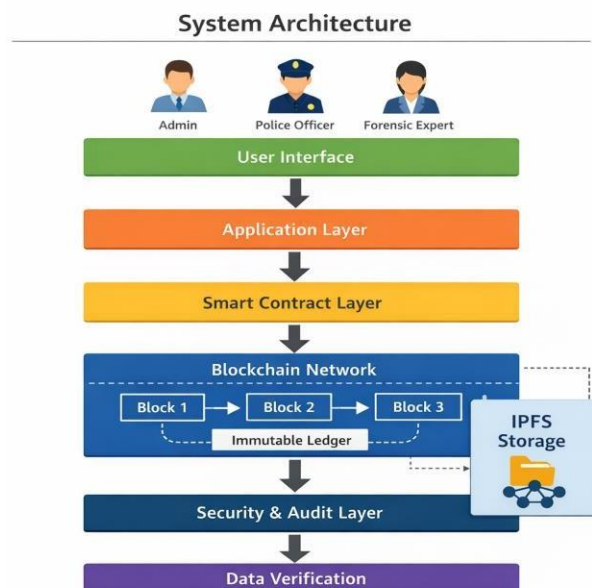
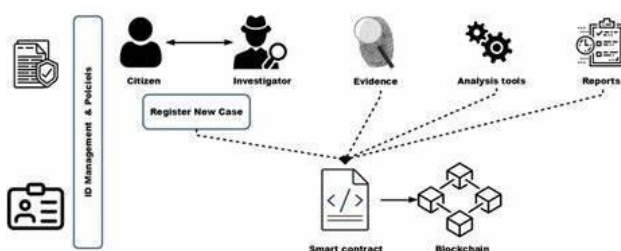
- Viewing and Monitoring

Admin and officers will have access to evidence and system logs at any given time. This is beneficial in tracing evidence and chain of custody.

Final Result

Any evidence is made safe, transparent and unalterable. This enhances confidence in police investigation and assists in provision of fair justice.

IV. SYSTEM ARCHITECTURE



V. WORKFLOW

The workflow describes the flow of criminal evidence within the system during its collection to confirmation. It demonstrates that blockchain secures evidence and makes it tamper resistant.

- User Registration

To begin with, every user such as Admin, Police Officers, and Forensic Experts sign up to the system. They include such information as name, ID, position. This assists in the identification of authorized users.

- User Login

The users are required to use username and password. The system identifies credentials and then approves access. This helps avoid unauthorized access. Admin Opening Officer Accounts. Admin includes the officer information like the police station and position. The officers are provided with a login that they can use to access the system. This assists in the safety of managing users. Crime Has Happened, Collection of Evidence. When a crime occurs, the police officers gather

evidence in the form of photos, videos, fingerprints, or documents. The evidence is ready to be uploaded into the system.

- Evidence Upload to System

Evidence is uploaded by the application through officer. IPFS storage is used to store large files. The file is given a distinct hash value.

- Smart Contract Check

Smart contracts verify the officer permission. Evidence information is documented in case of approval. This will provide automatic security.

- Blockchain Recording

Blockchain blocks contain evidence hash, officer ID, timestamp and case details. After data is stored it cannot be modified. This makes evidence unalterable.

- Chain of Custody Tracking

All the procedures such as the viewing, transferring, or updating of evidence are captured. This indicates the evidence handlers and their time. This is significant to court evidence.

- Access to Evidence by Authorized persons.

Evidence can be accessed by the officers, forensic experts or the administrator provided permission is given. The logs of all accesses are stored in blockchain.

- Evidence Verification

File hash is compared with blockchain hash. In case of a match - evidence is original. If not - tampering is detected.

- Monitoring & Reporting

Admin traces system logs and evidence. One can create reports to be investigated and presented to the court.

- Final Secure Storage

There is a permanent provision of evidence and its protection. This enhances faith, openness and justice system equity.

VI. ALGORITHMS

- Hashing Algorithm

The evidence files are given a distinct code through the hashing algorithm. In case an officer posts evidence such as an image or a video, the system will create a hash value of that file. In case an individual alters the file at a later point the hash value will be different and the system will not be fooled. This is to preserve evidence as original.

- Consent Algorithm in blockchain.

Blockchain operates on the consensus algorithm to ensure that all the nodes are in agreement before new evidence data can be added. The blockchain contains only validated and proper information. This eliminates the possibility of fake or unauthorized evidence being included and increases confidence in the system.

- Smart Contract Algorithm

Smart contracts refer to automatic programs that are written in Solidity and manage evidence operations. They verify regulations such as who is allowed to upload, view or transfer evidence. The action is permitted in case the user has the permission. This makes the system secure and automatic and it minimizes human error.

- Encryption Algorithm

Sensitive evidence data is encrypted in case they fall into the hands of hackers or unauthorized individuals. Evidence is transformed into secret message and it can be deciphered by authorized people only. This maintains privacy and secrecy of crime information.

- Digital Signature Algorithm.

The identity of the officer uploading the evidence is checked with the help of digital signatures. The evidence is digitally signed by each officer, which demonstrates that evidence is the addition of a real and authorized individual. This brings trust and responsibility in the system.

- Content Addressing Algorithm of IPFS.

IPFS has content-based addressing which stores evidence files. A file is given a distinct hash ID and this ID is stored in blockchain. In case the file is modified, a new hash ID will be formed, and failure will be identified. This provides integrity and a safe storage of evidence.

VII. RESULT ANALYSIS

With the introduction of Criminal Evidence Management System with the help of Blockchain, the system was successfully working and the criminal evidence was stored safely. Officers uploaded evidence in blockchain, where it was stored as hash values and timestamps. This made it impossible to tamper or delete evidence without anyone noticing it.

Other modules such as Admin Login, Officer Login, Add Officer, Add Evidence and View Evidence were also functional during testing. The officers could upload evidence files, documents, and images, and admins could see all the records. All the activity was documented as blockchain logs with indicators of block number and transaction ID among other details.

Any change in evidence was also detected using hash comparison by the system. In case the file has been altered, the hash value was not the same, and malpractice was immediately detected. This demonstrated that blockchain storage is safe and dependable to store criminal evidence.

Based on the analysis, the system registered numerous improvements compared to the traditional systems. It was more secure, transparent and trustworthy. Evidence could

be accessed by authorized people safely and chain of custody was allowed automatically. The system eliminated human mistakes and enhanced efficiency of investigations.

The general findings indicated that the evidence management system using blockchain is efficient, safe, and applicable to the police departments and court in handling the criminal evidence appropriately.

VIII. DISCUSSION

The Blockchain-based Criminal Evidence Management System demonstrates how the current technology can enhance the process of criminal evidence storage and handling by the police. In the conventional systems, the evidence is stored in central databases, which can be modified, deleted or lost. This poses difficulties in investigation and can give false verdicts. The suggested system addresses these issues with the help of blockchain that preserves evidence and makes it resistant to any manipulations.

In the course of work, we have seen that blockchain technology enhances security and transparency. Each operation such as evidence upload, access, or transfer is properly recorded forever with hash and timestamp. This assists in maintaining the chain of custody and makes the evidence credible in the court. Smart contracts were also useful in automating access control, therefore only authorized users could manipulate evidence.

There were some practical challenges also evident in the system. To manage blockchain, one will need more storage space, high computing power, and technical expertise. Moreover, big evidence files do require additional storage such as IPFS that complicates the system. The performance can also be impacted by network speed and costs of blockchain transactions.

Despite these difficulties, the system is quite convenient in the further law enforcement. It enhances the security of the data, decreases the human factor, and raises the confidence of people in the criminal investigations. As the issues related to blockchain-based evidence management are improved and the infrastructure is enhanced, it may become common in the police departments and the courts.

IX. CONCLUSION

The Criminal Evidence Management System with Blockchain is a safe and reliable mechanism to store and manipulate criminal evidence. In conventional systems, the evidence may be altered, lost or misused due to the fact that the evidence is stored in central databases. The problem is addressed in this project through the adoption of blockchain technology that secures evidence, which is considered permanent, safe, and unaffected.

Under this system, all evidence records are recorded with a hash value and a time. Smart contracts regulate access to evidence addition or access and all operations are automated. This will aid in preservation of the chain of custody and enhance confidence in the police investigations and court cases.

The findings indicate that the system is successful and enhances security, transparency, and accountability. Evidence is safe and any effort to alter evidence can be realized at once by the admin as well as officers. This ensures that the justice process is less biased.

Altogether, evidence management on blockchain is an effective technology of the future police structures. It can serve as a common tool in the police department, forensic laboratory, and courts with more enhancement in order to deliver justice appropriately.

X. FUTURE WORK

The Criminal Evidence Management System based on Blockchain may be enhanced in numerous aspects in the future. Enhancing the encryption and privacy practices with more resilient encryption and privacy measures to secure sensitive evidence data is one of them. Such technologies as high-level cryptography can ensure the safety of evidence and provide verification at the same time.

The other solution that can be used in future is the integration of Artificial Intelligence and Machine Learning. AI can assist police to automatically sort evidence, identify fake evidence, and identify helpful information at a faster rate. This will make investigations fast and more precise.

APIs can also be used to connect the system with other police and court systems. This will enable various departments to exchange evidence with ease and collaborate with each other. It will enhance interaction between courts, police and forensic labs.

Scalability and performance are also areas that need to be improved in the future. The system should be able to accommodate such large data without becoming slow as the volume of digital evidence grows. It will be beneficial to use improved blockchain platforms and storage techniques.

On the whole, having these advancements during the period the blockchain-based system of evidence management will become more robust, quicker, and more prevalent within the context of the law enforcement and the judicial system in the real world.

XI. REFERENCES

- [1] Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- [2] Vitalik Buterin (2014). *Ethereum White Paper*.
- [3] Juan Benet (2014). *IPFS – Content Addressed, Versioned, P2P File System*.
- [4] Christidis, K., & Devetsikiotis, M. (2016). *Blockchains and Smart Contracts for IoT*. IEEE Access.
- [5] Bashir, I. (2017). *Mastering Blockchain*. Packt Publishing.
- [6] Sharma, A., & Chen, M. (2019). *Blockchain-Based Digital Evidence Management System*.
- [7] Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy Using Blockchain*.
- [8] Tian, F. (2017). *Blockchain-Based Supply Chain Traceability System*.
- [9] Wüst, K., & Gervais, R. (2018). *Do You Need a Blockchain?*
- [10] Alharby, M., & van Moorsel, A. (2019). *Blockchain-Based Smart Contracts Mapping Study*.
- [11] Jayaraman, R., & Krishnan, A. *Blockchain for Forensic Evidence Chain-of-Custody Integrity*.

- [12] Agarwal, S., Jain, A., & Kumar, N. *SecureChain Framework for Digital Evidence Sharing.*
- [13] Atlam, H. F., & Wills, G. B. *Blockchain-Based Chain of Custody for Digital Evidence.*
- [14] Abbas, H. M., & Qamar, U. *Blockchain Technology for Digital Evidence Management.*
- [15] Dorai, G., & Sambasiva Rao, V. *EviBot: Blockchain-Powered Evidence Management.*